FY 13 Q3

Chief Information Officer

Federal Information Security Management Act

Reporting Metrics

Prepared by:

US Department of Homeland Security

Office of Cybersecurity and Communications

Federal Network Resilience

November 30, 2012

GENERAL INSTRUCTIONS

The majority of the FY13 Q3 metrics are based on the Administration Priorities. Please see the table below depicting the questions that are aligned to the Administration Priorities.

Administration Priority Area	Section	Performance Metric	Minimal Level for 2013	Target Level for 2013
Continuous[1] Monitoring – Assets	1.2	% of assets in 1.1, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets.	80%	95%
Continuous Monitoring – Configurations	2.1.2	% of the applicable hardware assets (per question 1.1), of each kind of operating system software in 2.1, that has an automated capability to identify deviations from the approved configuration baselines identified in 2.1.1 and provide visibility at the organization's enterprise level.		
Continuous Monitoring – Vulnerabilities	3.1	% of hardware assets identified in section 1.1 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.		
Identity Management HSPD-12	4.2, 4.3, 6.2	% of ALL people required to use Personal Identity Verification (PIV) Card to authenticate.	50%	75%
Boundary Protection CNCI[2] #1	5.2	% of external network traffic passing through a Trusted Internet Connection (TIC).[3]	80%	95%
Boundary Protection CNCI #1 & #2	5.1	% of required TIC capabilities implemented by TIC(s) used by the organization.	95%	100%

Table 1 – Administration Priorities Performance Metrics

[1] Continuous does not mean instantaneous. NIST SP 800-137 says that the term "continuous" means "that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information."

[2] Comprehensive National Cybersecurity Initiative (CNCI)

[3] Not applicable to Department of Defense (DoD).

1. Asset Management

1.1. What is the total number of organization hardware assets connected to the organization's unclassified[4] network(s)?[5] (Base)

1.2. What percentage of assets in 1.1 have an automated capability (scans/device discovery processes) to provide enterprise-level visibility into asset inventory information for all hardware assets? (AP)

1.3. For what percentage of applicable assets in 1.1 has the organization implemented an automated capability to detect and block unauthorized software from executing, or for what percentage does no such software exist for the device type? This may include software whitelisting tools that identify executable software by a digital fingerprint and selectively block these. It might also include sandboxing of mobile code to determine before execution whether to allow it to run, where static files do not allow whitelisting. In general, any method included should be able to block zero-day and APT threats. (KFM)

2. Configuration Management

2.1. For each operating system vendor, product, version,[6] and patch-level,[7] report the following:

2.1.1. Has an adequately secure configuration baseline been defined?[8] (KFM)

2.1.2. How many hardware assets (which are covered by this baseline, if it exists) have this software? (KFM)

2.1.3. What percentage of the applicable hardware assets (per question 1.1) of each kind of operating system software in 2.1 have an automated capability to identify deviations from the approved configuration baselines identified in 2.1.1 and provide visibility at the organization's enterprise level? (AP)

---

[4] "Unclassified" means low-impact (non-SBU) and SBU networks. Some organizations incorrectly use "unclassified" to mean not classified and not SBU.

[5] Unless specified otherwise in a footnote, add numbers across networks and organizational components to get the reportable result.

[6] Major versions only.

[7] Knowing version and patch-level is critical to knowing the CVEs these operating systems have and defining secure configuration baselines and what machines should use those baselines.

[8] "Defined" may include a narrative definition of the desired configuration. In the future, we will expect these standards to be defined directly as (a) data or (b) a test (preferably automated) of the configuration. Consider an organization-approved deviation as part of the organization standard security configuration baseline.

3. Vulnerability Management

3.1. How many hardware assets in 1.1 are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level? (AP)

4. Identity and Access Management

4.1. How many people have unprivileged network accounts? (Exclude privileged network accounts and non-user accounts.) (Base)

4.2. What percentage of people with an *unprivileged* network account are required to log onto the network by using a two-factor PIV card? (AP)
This metric measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication.

- Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced.
- Percentage should measure people because a person may have multiple accounts.
- For a person with more than one unprivileged network account, the person should be counted in the percentage only if the person is required to use a two-factor PIV card to authenticate to all accounts.

4.3. How many people have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.) (Base)

4.4. What percentage of people with a *privileged* network account is required to log onto the network by using a two-factor PIV card? (AP)
This metric measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication.

- Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced.
- Percentage should measure people because a person may have multiple accounts.
- For a person with more than one privileged network account, the person should be counted in the percentage only if the person is required to use a two-factor PIV card to authenticate to all accounts.

4.5. Please provide the working URL to the agency's progress update for HSPD-12 implementation.

4.6. List all major IT investments as reported to OMB per M-11-11 and answer the following questions for each investment:

UPI (2012) (17–digits required for all legacy investments)	Bureau Code	Planning (0=No; 1=Yes)	Development (0=No; 1=Yes)	Operations (0=No; 1=Yes)	Investment Title	Are all systems associated with this investment PIV-enabled in accordance with OMB policy (e.g. M-10-15, M-11-11) and NIST standards and guidelines? (0=No; 1=Yes; 3=N/A)

5. Boundary Protection

5.1. What percentage of the required TIC 2.0 Capabilities is implemented? (AP)

Instruction: Question 5.2 applies only to Federal civilian organizations. If the reporting organization is not a Federal civilian agency, answer N/A to these questions.

5.2. What percentage of external network traffic to/from the organization's networks passes through a TIC/MTIPS? (AP)

5.3. Is the organization's internet service (whether obtained through a TICAP or other means) configured to manage filters, excess capacity, or bandwidth or provide other redundancies to limit the effects of information-flooding types of denial-of-service attacks on the organization's internal networks and internet services? Such configuration may include agreements with external network operators to reduce the susceptibility to these types of attacks and respond to them. (Base)

5.4. What percentage of the Agency's Federal facilities uses card readers for physical access? (Base)

5.5. What percentage of those facilities with card readers is HSPD-12 compliant? Note: It is recognized that where facilities are leased from GSA, these metrics are not entirely controlled by the Tenant (i.e., the Agency). (Base)

5.5.1. For facilities with 1,000 or more users: What percentage of the facilities uses card readers for physical access?

5.5.2. For facilities with 1,000 or more users: What percentage of the facilities uses HSPD-12-compliant card readers?

5.5.3. For facilities with less than 1,000 users: What percentage of the facilities uses card readers for physical access?

5.5.4. For facilities with less than 1,000 users: What percentage of the facilities uses HSPD-12-compliant card readers?

6. Remote Access

6.1. How many people log onto the organization's remote access solution(s) to obtain access to the organization's desktop LAN/WAN resources or services? (Base)

6.2. For remote access, what percentage of people are required to log onto the organization's desktop LAN/WAN resources or services by using a two-factor PIV card? (AP)
This metric measures the percentage of people who are required to log on using a two-factor PIV card as the normal mode of authentication for remote access.

- Percentage should include people currently using temporary credentials if the person's normal mode of authentication is PIV-enforced.
- Percentage should measure people because a person may have multiple accounts.
- For a person with more than one account, the persons should be counted in the percentage only if the person is required to use a two-factor PIV card to authenticate to all accounts.

7. Enterprise Security Architecture

7.1. How is the organization's enterprise security architecture process integrated with its implementation of the DHS CEASARS architecture and the organization's overall risk management process? (Base)

7.2. How does the architecture process contribute to the overall risk management process? (Base)

7.2.1. How could the architecture process be improved to better contribute? (Base)

7.3. Has the organization identified first-priority risks that are not addressed by the architecture? (Base)

7.4. What processes are used to identify whether the Agencies have links to the organization's enterprise architecture at the system, segment, and enterprise levels? (Base)

7.4.1. Does the organization's architecture provide context, standards, and consistency across the FISMA areas that are being measured? (Base)

7.4.2. Is the organization referencing the NIST Risk Management Framework? If so, how? (Base)

7.5. How does the organization build security governance, requirements, and models into the Enterprise Architecture Process to provide an actionable blueprint? (Base)